

Protection of Personal Information Policy

Objective

The Protection of Personal Information Policy sets out the objectives for the legal processing of personal information within the Canal West Home Owners Association (herein referred to as "The Association", which includes its trustees and employees).

Scope

The scope of the Protection of Personal Information Policy covers the day to day management functions of The Association. These may include (but not limited to):

- Send levy accounts and statements to the correct people;
- Allocate payments correctly;
- Send out communications about the annual budget and financial statements, the Annual General Meeting (AGM) and other Home Owners Association (HOA) matters and/or meetings;
- Deal with building applications from Home Owners as well as the non-compliance of The Association's building regulations – both with the support of The Association's Resident Architect;
- Facilitate communications with owners and tenants regarding community matters, security issues or in an emergency such as the recent Covid-19 lockdown;
- Issue warning letters and/or fines for any non-adherence of The Association's Constitution and Rules; and
- Take swift action in the event of levy defaults, including the hand-over of bad debtors to a Legal Professional for legal collection.

Policy

1. The Association is committed to compliance with the Protection of Personal Information Act ("POPIA") which requires it to protect any personal information it collects.
2. This policy establishes the principles for the protection and lawful processing of personal information within our organisation and the rights of individuals to privacy and to reasonable safeguarding of their personal information.
3. All employees, trustees and individuals directly associated with The Association are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.
4. Any third-party service providers to The Association must adhere to the requirements of POPIA to ensure the adequate protection of personal information held by them on behalf of The Association.
5. Policy Principles
 - 5.1. Principle 1: Accountability
 - 5.1.1. We must take reasonable steps to ensure that personal information obtained from data subjects is stored safely and securely.
 - 5.2. Principle 2: Processing Limitation

- 5.2.1. We will collect personal information directly from data subjects.
- 5.2.2. We will only process personal information with consent, where we are required to do so by law or in the legitimate interest of the data subject.

5.3. Principle 3: Specific Purpose

- 5.3.1. We collect personal information from data subjects in order to provide them with services related to The Association.

5.4. Principle 4: Limitation on Further Processing

- 5.4.1. Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially.

5.5. Principle 5: Information Quality

- 5.5.1. We are responsible for ensuring that personal information is complete, up to date and accurate before we use it. This means that it may be necessary to request the data subjects, from time to time, to update their information and confirm that it is still relevant.

5.6. Principle 6: Transparency/Openness

- 5.6.1. Where personal information is collected from a source other than directly from a data subject we are responsible for ensuring that the data subject is aware:
 - 5.6.1.1. That their information is being collected;
 - 5.6.1.2. Who is collecting their information by giving them our details and informing them of the specific reason for collecting their information.

5.7. Principle 7: Security Safeguards

- 5.7.1. We will ensure that technical and organisational measures are in place to secure the integrity of personal information, and guard against the risk of loss, damage or destruction thereof. Personal information must also be protected against any unauthorised or unlawful access or processing.

5.8. Principle 8: Participation of Individuals

- 5.8.1. Data subjects are entitled to know particulars of their personal information held by The Association. They are also entitled to correct any information held on behalf of The Association.

6. Operational Considerations

6.1. Monitoring

- 6.1.1. The Information Officer is responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, procedures, notices, consents and appropriate related documents. All employees, trustees and individuals directly associated with The Association are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information. Periodic reviews and audits will be conducted, where appropriate, to ensure compliance with this policy and guidelines.

6.2. Operating controls

- 6.2.1. We shall establish appropriate procedures that are consistent with this policy and regulatory requirements. This will include:
 - 6.2.1.1. Allocation of information security responsibilities.
 - 6.2.1.2. Incident reporting and management.
 - 6.2.1.3. Information security education.
 - 6.2.1.4. Data backup.